UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/751,300	01/02/2004	Pasi Eronen	944-4.40	8800

4955 7590 10/04/2007
WARE FRESSOLA VAN DER SLUYS & ADOLPHSON, LLP
BRADFORD GREEN, BUILDING 5
755 MAIN STREET, P O BOX 224
MONROE, CT 06468

EXAMINER	
LE, CANH	
ART UNIT	PAPER NUMBER
2139	
MAIL DATE	DELIVERY MODE
10/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/751,300	**Applicant(s)** ERONEN ET AL.	
	Examiner Canh Le	**Art Unit** 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☒ Claim(s) *5* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Claims 1- 7 have been amended.

Claims 8-11 have been added.

Claims 1-11 have been examined and are pending.

Claim Objections

Claim 5 is objected to because of the following informalities: Claim 5 recites, "computer program product comprising a computer readable storage structure". It is unclear how computer program product including a computer readable storage structure. For example, A computer program product can be a piece of paper or a floppy disk. It is unclear that the floppy disk can include a computer readable storage structure. Appropriate correction is required.

Response to Arguments

Applicant's arguments filed 07/19/2007 have been fully considered but they are not persuasive.

With respect to claims 1 and 6, The Applicant argues that:

Dharmapurikar does not suggest using a Bloom filter in a RAND challenge, not determining that there is a match, and the combination of Patel and Dharmapurikar is not obvious.

The Office respectfully disagrees:

Dharmapurikar teaches a probabilistic data structure that is used to determine whether or not an element is a member of a set. "A Bloom filter is essentially a bit-vector of length *m* used to efficiently represent a set of messages. Given a set of messages *X* with *n* members, the Bloom filter is "programmed" as follows. For each message *xi* in *X*, *k* hash functions are computed on x_i producing *k* values each ranging from 1 to *m*. Each of these values address a single bit in the *m*-bit vector, hence each message x_i causes *k* bits in the *m*-bit vector o be set to 1. Note that if one of the *k* hash values addresses a bit that is already set to 1,that bit is not changed. Querying the filter for set membership of a given message *x* is similar to the programming process. Given message *x*, *k* hash values are generated using the same hash functions used to program the filter. The bits in the *m*-bit long vector at the locations corresponding to the *k* hash values are checked. If at least one of the *k* bits is 0,then the message is declared to be a non-member of the set. If all the bits are found to be 1,then the message is said to belong to the set with a certain probability" [pg. 203, Bloom Filter Theory section to pg. 204, section Counting Bloom filter].

Other the hand, Patel teaches that the client insist that RAND have to be different from each other. Patel teaches determining if there is a match between R_1 and R_2. "If three RANDs are used then insist that R1 and not equal R2 and R1 not equal R3, and R2 not equal R3" [pg. 2; section 2.1.2. Solutions].

In response to applicant's argument that there is no suggestion to combine the references, the Office recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). Dharmapurikar teaches the limitations which Patel does not teach such as determining whether or not an element is a member of a set while Patel teaches determining if there is a match between R_1 and R_2. Therefore, the combination of teaching between Dharmapurikar and Patel is proper and efficient.

With regard to claim 3, The Applicant argues:

Dharmapurika nowhere teaches or suggests using a RAND to set to one the value of one or another component of a data structure of ordered components.

The Office respectfully disagrees:

Dharmapurikar teaches a Bloom filter with a bit-vector of length m used to efficiently represent a set of messages. For each message x_i in X, k hash functions are computed on x_i producing k values each ranging from 1 to m. For each of these value address a single bit in the m-bit vector, hence each message x_i causes k bits in the m-bit vector to set to 1 [pg. 203, section 3.1 Bloom filter]. IP address is random number within a range such as a Dynamic Host Configuration Protocol (DHCP).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3 and 5-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Sarvar Patel,** "Analysis of EAP-SIM Session Key Agreement", IETF EAP mailing, May 29, 2003, pp. 1-4 in view of **Dharmapurikar et al.,** "Longest Prefix Matching Using Bloom Filter", SIGCOMM'03, August 25-29, 2003, pp. 201-212.

<u>As per claim 1:</u>

Patel teaches a method for use by a telecommunications terminal (10) in authenticating the telecommunications terminal (10) comprising **[pg. 1 to pg. 4]**:

Patel does not teach, "(a) encoding random numbers previously used ... one of the previously used random numbers; (b) checking the data structure (21) to determine whether a candidate random number is not one of the previously used random numbers; (c) wherein the data structure (21) is such as to at least provide a true answer as to whether the candidate random number is not one of the previously used random numbers".

However, Dharmapurikar teaches:

(a) encoding random numbers previously used for authenticating the telecommunications terminal (10), so as to provide a data structure (21) consisting of an ordered set of components having respective component values derived from the previously used random numbers, wherein each component has a starting value of zero, but the value is set to one if, based on the order of the component in the ordered set, the component is pointed to by any of a plurality of pointer values each based on all the bits of a respective one of the previously used random numbers **[pg. 203, Bloom Filter Theory section to pg. 204, section Counting Bloom filter]**; and

(b) checking the data structure (21) to determine whether a candidate random number is not one of the previously used random numbers **[pg. 203, Bloom Filter Theory section to pg. 204, section Counting Bloom filter]**;

(c) wherein the data structure (21) is such as to at least provide a true answer as to whether the candidate random number is not one of the previously used random numbers [**pg. 203, section 3. BLOOM FILTER THEORY to pg. 204, section 3.2 Counting Bloom Filters; "If at least one of the k bits is 0, then the message is declared to be a non-member of the set"]**.

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Patel of the invention by including the step of Dharmapurikar because It would provide efficient using Bloom filter which is an efficient data structure for membership queries with tunable false positive errors **[Dharmapurikar, pg. 201, col. 2, par. [2], lines 1-5].**

As per claim 2:

Dharmapurikar teaches a method as in claim 1, wherein in encoding the previously used random numbers, a set of hash functions is used each providing a value in a range equal to the number of components of the data structure (21), and for each previously used random number, each of the hash functions is evaluated and the component in the ordered set of components at the position indicated by the hash function value is set to one **[pg. 203, section 3. BLOOM FILTER THEORY to pg. 204, section 3.2 Counting Bloom Filters; "For each message x_i in X ... m-bit causes k bits in the m-bit vector to be set to 1"]**.

As per claim 3:

Dharmapurikar teaches a method as in claim 1, wherein in encoding the previously used random numbers, the previously used random numbers are used as the pointer values **[pg. 203, section 3. BLOOM FILTER THEORY to pg. 204, section 3.2 Counting Bloom Filters; "For each message x_i in X ... m-bit causes k bits in the m-bit vector to be set to 1"; pg. 211, fig. 10a; H1 is a pointer which point to m bits vectors of Boom filter]**.

As per claim 5:

Claim 5 is essentially the same as claim 1 except that it sets forth the claimed invention as a computer program product rather a method and rejected under the same reasons as applied above.

As per claim 6:

Claim 6 is essentially the same as claim 1 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

As per claim 7:

Claim 7 is essentially the same as claim 1 except that it sets forth the claimed invention as a system rather a method and rejected under the same reasons as applied above.

As per claim 8:

Patel teaches an apparatus for use by a telecommunication terminal (10) in authenticating the telecommunications terminal (10) to an access network, comprising an authenticator module (14) **[pg. 1 to pg. 4].**

Patel does not teach, "one or more Bloom filter modules (11 12), configured to: (a) encode random numbers previously used for authenticating.. (b) check the data structure (21) to determine.. (c) wherein the data structure (21) is such as to at least provide a true answer as to whether the candidate random number is not one of the previously used random numbers".

However, Dharmapurikar teaches: one or more Bloom filter modules (11 12), configured to:

(a) encode random numbers previously used for authenticating the telecommunications terminal (10), so as to provide a data structure (21) consisting of an ordered set of components having respective component values derived from the previously used random numbers, wherein each component has a starting value of zero, but the value is set to one if, based on the order of the component in the ordered set, the component is pointed to by any of a plurality of pointer values each based on all the bits of a respective one of the previously used random numbers **[pg. 203, Bloom Filter Theory section to pg. 204, section Counting Bloom filter]**; and

(b) check the data structure (21) to determine whether a candidate random number is not one of the previously used random numbers **[pg. 203, Bloom Filter Theory section to pg. 204, section Counting Bloom filter]**;

(c) wherein the data structure (21) is such as to at least provide a true answer as to whether the candidate random number is not one of the previously used random numbers [**pg. 203, section 3. BLOOM FILTER THEORY to pg. 204, section 3.2 Counting Bloom Filters; "If at least one of the k bits is 0, then the message is declared to be a non-member of the set"]**.

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Patel of the invention by including the step of Dharmapurikar because It would provide efficient using Bloom filter which is an efficient data structure for membership queries with tunable false positive errors **[Dharmapurikar, pg. 201, col. 2, par. [2], lines 1-5].**

<u>As per claim 9:</u>

Dharmapurikar teaches an apparatus as in claim 8, wherein for encoding the previously used random numbers the authenticator module (14) and one or more Bloom filter modules (11 12) are configured so that a set of hash functions is used each having a range equal to the number of components of the data structure (21), and for each previously used random number, each of the hash functions is evaluated and the component in the ordered set of components at the position indicated by the hash function value is set to one **[pg. 203, section 3. BLOOM FILTER THEORY to pg. 204, section 3.2 Counting Bloom Filters; "For each message x_i in X ... m-bit causes k bits in the m-bit vector to be set to 1"]**.

<u>As per claim 10:</u>

Claim 10 is essentially the same as claim 3 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

Claims 4 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Sarvar Patel**, "Analysis of EAP-SIM Session Key Agreement", IETF EAP mailing, May 29, 2003, pp. 1-4 in view of **Dharmapurikar et al.,** "Longest Prefix Matching Using Bloom 7Filter", SIGCOMM'03, August 25-29, 2003, pp. 201-212 and further in view of **Aguilera et al.** (US 2005/002209 A1).

As per claim 4:

Dharmapurikar teaches a method as in claim 1, wherein the data structure (21) is a multi-part data structure (21) with each part having an upper limit on the number of random number values it can indicate as one of the previously used random number values wherein each part has values based on only some of the previously used random numbers, and wherein all most recently received random numbers are used in determining component values in only one of the parts **[pg. 211, fig. 10b; there are Bloom Filters of length m/2]**.

Patel and Dharmapurikar do not explicitly teach an upper limit is reached for the one of the parts, another of the parts is reset.

However, Aguilera teaches teach an upper limit is reached for the one of the parts, another of the parts is reset **[par. [0014], lines 8-14].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Patel and Dharmapurikar of the invention by including the step of Aguilera because It would provide a simple solution that would be to reset the Bloom filter to an empty state **[Aguilera, par. [0014], lines 12-13].**

As per claim 11:

Claim 11 is essentially the same as claim 4 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

Action is Final

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le

September 22, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100